

ABSTRACT

In a method for authorizing a transaction by a user with the aid of a terminal which can communicate with a background system, a secret, which is known to the user and to the background system but not to an unauthorized attacker, is used. The background system transmits secret data, which indicate the secret, only to the terminal if the terminal has successfully authenticated itself at the background system. Because, as a rule, secret data of several users are stored in the background system, the terminal detects in advance identification information which identifies the user, and transmits corresponding user identification data to the background system. When the terminal displays the secret to the user, the user can be certain that the terminal is trustworthy. A device and a computer program product comprise corresponding features. The invention provides a technique for authorizing a transaction by a user with the aid of a terminal which enables the user to recognize a falsified terminal.

15